IDENTITY PROTECTION

By John D Woodward Jr, Director of the Department of Defense Biometrics Management Office

The Department of Defense has long emphasized using state-of-the-art technology to secure and protect its most vital assets – people, information and equipment. Specifically, DoD has been a leader in the United States government in the following three technologies.

- Smart card technology – DoD's version, the Common Access Card (CAC), is currently held by more than three million DoD civilians and contractors worldwide.
- Public key infrastructure (PKI) – DoD uses PKI for network logon, digital signing, and encryption of e-mail communications.
- Biometrics – This term refers to measurable physical characteristics or personal traits used to recognize the identity or verify the claimed identity of an individual.

Each of these technologies is a tool that can help manage and protect an individual's identity throughout his/her association with DoD. Moreover, these tools can be used to complement each other and to provide military commanders with security options for applications. The technologies' synergy led the DoD Chief Information Officer (CIO) to change the department's approach to managing and overseeing these three programs. On January 12, 2004, the DoD CIO took the first step to create an integrated, enterprise-wide approach to identity management when he formed the DoD Identity Protection and Management Senior Coordinating Group (IPMSCG).

FORMATION OF THE IPMSCG

The IPMSCG serves as the senior oversight body for the management of the department's smart card, PKI, and biometrics programs. Previously, three separate senior bodies were responsible for these three programs. The IPMSCG merges the Smart Card Senior Coordinating Group, Public Key Infrastructure Senior Steering Committee, and the Biometrics Senior Coordinating Group into one senior oversight body. The IPMSCG consists of general officer and senior civilian representatives from each of the armed forces, joint staff, the Office of the Secretary of Defense, and DoD organizations. The IPMSCG focuses on ways to use identity management tools while protecting an individual's privacy.

In his January 12 memorandum, the DoD CIO explained that the IPMSCG "shall be a cohesive DoD-wide policy, requirements, strategy, and oversight group for managing the physical and virtual identities of all our personnel, support contractors, business partners, and other entities consistent with the Global Information Grid Architecture".

The DoD defines the Global Information Grid as the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war-fighters, policy makers, and support personnel.

Serving as the IPMSCG Chair, the Department of the Navy CIO David Wennergren, has announced three main priorities for the IPMSCG:

- To develop an overarching identity management vision that will encompass more than the sum of the three programs.
- To identify the right set of tasks in order to achieve that vision, focusing on execution and driving near-term results.
- To obtain business results by eliminating duplication and disparities of effort across the three programs.

BIOMETRICS: NEW IDENTITY MANAGEMENT TOOL

While the Common Access Card and PKI have been deployed as successful identity management solutions for DoD, biometric technologies are a relative newcomer to this arena. When the DoD biometrics program started in 2000, it emphasized the use of biometrics for logical access to computers, networks and information systems. Following

the events of September 11, 2001, the focus shifted to supporting US efforts in the global war on terrorism. The US military has always faced the challenge of identifying 'friend or foe'. Now, the challenge is made all the more difficult as we face a highly mobile terrorist foe, deliberately engaging in tactics to conceal true affiliation and allegiance. Biometrics are a tool that can help US authorities recognize national security threats.

NEED FOR INTEROPERABILITY

The DoD CIO's vision is for the IPMSCG to "focus on department-wide interoperability standards, performance matrices, and ways to exploit identity management tools as means for enhancing readiness, business processes and security, while also being cognizant of protecting entities' identifiable information".

Interoperability is particularly important as DoD moves towards greater net-centricity. IPMSCG stakeholders will also look as needed to government organizations outside of DoD to facilitate greater identity management system interoperability.

SETTING THE COURSE FOR DOD IDENTITY MANAGEMENT

After receiving comments from stakeholders, the IPMSCG will finalize its governing charter this summer. Specific elements will likely include:

- Ensuring DoD-wide coordination of identity management functional capabilities, strategies and objectives.
- Developing outcome-based performance metrics for identity management solutions.
- Briefing external authorities on identity management issues.
- Ensuring privacy issues are addressed in the department's identity management efforts.

The IPMSCG will receive technical and administrative support from the DoD Biometrics Management Office, DoD Access Card Office, and DoD PKI Program Management Office for their respective focus areas. The IPMSCG plans to meet at least four times a year. In addition, numerous working group meetings will be held.

In summary, the IPMSCG will develop a corporate vision for identity protection and management within the DoD. This vision will draw heavily on the enabling tools of the Common Access Card, PKI and biometric technologies. ■